REMOTE MONITOR SYSTEM

Patent Number: JP11161517

Publication date: 1999-06-18

Inventor(s): YAMAMOTO ATSUSHI

Applicant(s): MEIDENSHA CORP

Requested Patent: JP11161517

Application Number: JP19970325538 19971127

Priority Number(s):

IPC Classification: G06F11/30; G05B23/02; G06F9/06; G06F12/14

EC Classification:

Equivalents:

Abstract

PROBLEM TO BE SOLVED: To prevent infection with viruses and to prevent the loss of a monitoring function in the case of turning a personal computer to a central processing unit and monitoring and further controlling an equipment through an input/output device.

SOLUTION: In this system for connecting the central processing units 11 and 12 and the input/output devices 61 - 6N by 'Ethernet (R)', the central processing units 11 and 12 are provided with a performance monitoring application 5 for performing monitoring for the file size of the respective kinds of applications 2 and 3 and resources managed by an OS 4. The input/output devices 61 -6N are provided with an abnormality judgement function 12 for judging whether or not the central processing units are infected with the viruses from the data monitored by the performance monitoring application 5 and automatically executing a virus coping program to all the central processing units 11 and 12 at the time of judging that they are infected with the viruses.

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－161517

(43)公開日　平成11年(1999)6月18日

(51)Int.Cl.[6]		識別記号	FI		
G06F	11/30		G06F	11/30	D
G05B	23/02	302	G05B	23/02	302 J
G06F	9/06	550	G06F	9/06	550 Z
	12/14	310		12/14	310 Z

審査請求　未請求　請求項の数2　OL　（全4頁）

(21)出願番号　特願平9-325538

(22)出願日　平成9年(1997)11月27日

(71)出願人　000006105
株式会社明電舎
東京都品川区大崎2丁目1番17号

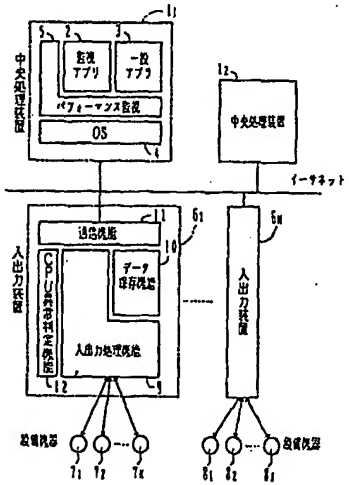
(72)発明者　山本　厚史
東京都品川区大崎2丁目1番17号　株式会社明電舎内

(74)代理人　弁理士　志賀　富士弥　（外1名）

(54)【発明の名称】遠方監視システム

(57)【要約】
【課題】　パーソナルコンピュータを中央処理装置とし、入出力装置を通して設備機器の監視さらには制御をする遠方監視システムにおいては、ウイルスに感染し易く、監視機能を喪失することがある。
【解決手段】　中央処理装置1_1，1_2と入出力装置6_1～6_Nをイーサネットで接続するシステムにおいて、中央処理装置は搭載する各種アプリケーション2，3のファイルサイズ及びOS4が管理する資源について監視を行うパフォーマンス監視アプリケーション5を設ける。入出力装置は、パフォーマンス監視手段が監視するデータから中央処理装置がウイルスに感染したか否かを判定し、ウイルスに感染したと判定したときに全ての中央処理装置に対してウイルス対処プログラムを自動的に実行する異常判定機能12を設ける。

実施形態のシステム構成



【特許請求の範囲】
【請求項1】　パーソナルコンピュータを中央処理装置とし、入出力装置を通して設備機器の監視さらには制御をする遠方監視システムにおいて、
前記中央処理装置は、搭載する各種アプリケーションのファイルサイズ及びOSが管理する資源について監視を行うパフォーマンス監視手段を設け、
前記入出力装置は、前記パフォーマンス監視手段が監視するデータから中央処理装置がウイルスに感染したか否かを判定し、ウイルスに感染したと判定したときに全ての中央処理装置に対してウイルス対処プログラムを自動的に実行する異常判定手段を設けたことを特徴とする遠方監視システム。
【請求項2】　前記異常判定機能は、前記ウイルス対処プログラムの実行後もウイルス感染を判定したとき、前記中央処理装置が保存するデータの全てを外部媒体のデータで書替える手段を備えたことを特徴とする請求項1記載の遠方監視システム。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、遠方監視や制御を行う遠方監視システムに係り、特にパーソナルコンピュータを監視処理装置とするシステムのウイルス対策に関する。
【0002】
【従来の技術】遠方監視システムは、例えば変電所の監視には、所内各設備機器側の子局から監視室側の親局に監視情報を伝送し、親局側の監視処理装置で機器の状態等を監視する。制御機能も持つシステムでは、親局側から子局側に制御情報も伝送する。
【0003】親局側の監視処理装置は、その性格上、コンピュータを中枢部として構成され、コンピュータも技術の進歩やシステムの大規模化に伴いミニコンピュータからメインフレーム、さらにワークステーションと進化し、現在では低価格化と高機能化されたパーソナルコンピュータを採用するものが増えてきている。
【0004】パーソナルコンピュータは、ネットワークの接続やワープロ・ゲームなど多種多様な目的に使用できるため、その内部データ破壊を目的としたウイルスプログラムとの接触の機会が多く、ウイルスプログラムと接触したときには重大な障害を受けてしまう。
【0005】特に、パーソナルコンピュータが監視システムや監視制御システムの中枢部とされる場合、ウイルスプログラムに感染すると、コンピュータ動作への干渉や設備の監視や制御が不能になるなど、深刻な事態になってしまう。
【0006】ウイルスプログラムからの接触を避けるものとして、手動又はバッチファイル等を使って市販のウイルス対処プログラムを実行させる方法が採られている。
【0007】
【発明が解決しようとする課題】従来のウイルス対処方法では、ウイルス感染を人が感知し、ウイルスプログラムを実行することになる。
【0008】このため、監視室の運転員がウイルス感染にすぐ気づいて対応する事ができれば問題はないが、夜間など、人のいないときにウイルスによる不具合が発症したときには対応が遅れ、監視機能の喪失などシステムに深刻な結末となってしまう。
【0009】本発明の目的は、ウイルス感染及び不具合の発症を自動的に検知及び対処処理できる遠方監視システムを提供することにある。
【0010】
【課題を解決するための手段】本発明は、ウイルス感染の判定機能を設け、処理装置がウイルス感染したときに直ちにウイルス対処プログラムを自動的に実行するようにしたもので、以下の構成を特徴とする。
【0011】パーソナルコンピュータを中央処理装置とし、入出力装置を通して設備機器の監視さらには制御をする遠方監視システムにおいて、前記中央処理装置は、搭載する各種アプリケーションのファイルサイズ及びOSが管理する資源について監視を行うパフォーマンス監視手段を設け、前記入出力装置は、前記パフォーマンス監視手段が監視するデータから中央処理装置がウイルスに感染したか否かを判定し、ウイルスに感染したと判定したときに全ての中央処理装置に対してウイルス対処プログラムを自動的に実行する異常判定手段を設けたことを特徴とする。
【0012】また、前記異常判定機能は、前記ウイルス対処プログラムの実行後もウイルス感染を判定したとき、前記中央処理装置が保存するデータの全てを外部媒体のデータで書替える手段を備えたことを特徴とする。
【0013】
【発明の実施の形態】図1は、本発明の実施形態を示す監視システム構成図である。監視システムの中央処理装置1_1，1_2は、パーソナルコンピュータで構成される。装置1_1，1_2の内部アプリケーション構成は、装置1_1に代表して示すように、監視システムアプリケーション2や市販の一般のアプリケーション3とOS（オペレーティングシステム）4との間に、パフォーマンス監視アプリケーション5を備える。
【0014】パフォーマンス監視アプリケーション5は、パーソナルコンピュータにインストール（搭載）されている各種アプリケーション3，4のファイルサイズをデータベースとして保持する。また、アプリケーション5は、OS4と通信を行い、パーソナルコンピュータ内の資源についても監視を行う。
【0015】入出力装置6_1～6_Nは、イーサネット等を使った通信システムを通して装置1_1，1_2と結合される。これら入出力装置6_1～6_Nは、直接に又は子局を介

して監視対象又は監視制御対象となる各種の設備機器7_1～7_K、8_1～8_Jの状態信号の取り込み及び制御信号の出力を行い、中央処理装置1_1、1_2との間で情報授受を行う。

【0016】入出力装置6_1～6_Nのアプリケーション構成は、装置6_1に代表して示すように、アプリケーションとして設備機器との入出力処理機能9、データ保存機能10及び通信機能11の他に、CPU異常判定機能12を備える。

【0017】この異常判定機能12は、中央処理装置1_1、1_2のパフォーマンス監視アプリケーション5との間で通信を行い、アプリケーション5から取り込んだデータについてそのファイルサイズの変化や資源の変化からウイルスに感染したか否かを判定し、ウイルスに感染したと判定したときには中央処理装置1_1、1_2に対してウイルス対処プログラムを実行する。

【0018】このプログラムの実行は、例えば、中央処理装置1_1がウイルスに感染したと判定したときに該装置1_1に対してウイルス対処プログラムを実行すると共に、残りの中央処理装置1_2に対してもウイルス対処プログラムを実行する。

【0019】したがって、本実施形態によれば、中央処理装置1_1、1_2の少なくとも1台がウイルス感染したことを入出力装置6_1～6_Nの1つが判定したときに直ちに全ての中央処理装置に対して自動的にウイルス対処プログラムを実行する。

【0020】これにより、ウイルス感染を早期に判定し、設備機器の監視不能などの発症前にウイルス感染に対処できる。また、1台の中央処理装置のウイルス感染で全ての中央処理装置に対してウイルス対処プログラムを実行するため、他の健全な中央処理装置がウイルスに感染する前に対処できる。

【0021】なお、ウイルス対処プログラムの実行後、CPU異常判定機能12が再度ウイルス感染を検知したときは、中央処理装置内のすべてのデータを更新することで監視機能の確保を確実にすることができる。

【0022】例えば、図2に示すように、中央処理装置1_1がウイルス感染し、入出力装置6_1がウイルス対処プログラムを実行した後もCPU異常判定機能12がウイルス感染を検知したとき、中央処理装置1_1に接続された外部媒体13に対して書替え指令を発生し、中央処理装置1_1内のハードディスクの全てのデータファイルを健全なものに書替える。

【0023】

【発明の効果】以上のとおり、本発明によれば、ウイルス感染の判定機能を設け、処理装置がウイルス感染したときに直ちにウイルス対処プログラムを自動的に実行するようにしたため、ウイルス感染の自動検知及び発症前にウイルス対処プログラムの実行ができ、夜間など人のいないときにウイルスに感染するも監視機能の確保を確実にすることができる。

【図面の簡単な説明】

【図1】本発明の実施形態を示すシステム構成図。

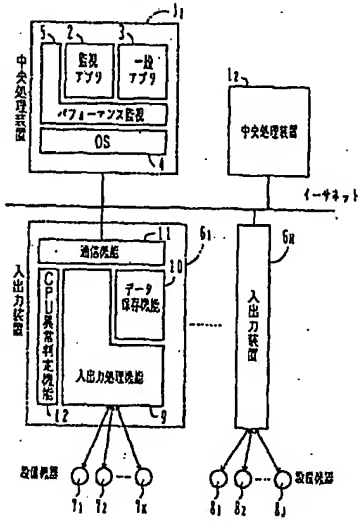
【図2】実施形態におけるデータ書替え処理。

【符号の説明】

1_1、1_2…パーソナルコンピュータ構成の中央処理装置
2…監視アプリケーション
3…一般アプリケーション
4…OS
5…パフォーマンス監視アプリケーション
6_1、6_N…入出力装置
7_1～7_K、8_1～8_J…設備機器
9…入出力処理機能
10…データ保存機能
11…通信機能
12…CPU異常判定機能
13…外部媒体

【図1】

実施形態のシステム構成



【図2】

実施形態のデータ書替え処理